UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

COURTNEY DIANA individually and on behalf of all others similarly situated, Plaintiff, v. HORIZON HEALTHCARE SERVICES, INC., d/b/a HORIZON BLUE CROSS BLUE SHIELD OF NEW JERSEY, a New Jersey corporation, Defendant.	Case No. 2:13-CV-07418-CCC-MF
KAREN PEKELNEY, MARK MEISEL, and MITCHELL RINDNER, on behalf of themselves and all others similarly situated, Plaintiffs, v. HORIZON HEALTHCARE SERVICES, INC., d/b/a HORIZON BLUE CROSS BLUE SHIELD OF NEW JERSEY, a New Jersey corporation, Defendant.	Case No. 2:14-cv-00584-CCC-MF

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Courtney Diana, Karen Pekelney, Mark Meisel, and Mitchell Rindner ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their attorneys, hereby bring this Consolidated Class Action Complaint against Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey ("Horizon" or "Defendant").

NATURE OF THE CASE

1. This is a consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all others similarly situated (*i.e.*, the Class Members), who are consumers of health insurance coverage and entrusted Horizon to safeguard their (1) personally identifiable information ("PII"), which includes without limitation members' names, dates of birth, Social Security numbers, and addresses; and (2) protected health information ("PHI"), which contains PII in addition to members' demographic information, medical histories, test and laboratory results, insurance information, and other data collected by health care professionals to identify an individual and determine appropriate care.

2. Two unencrypted laptops at Horizon's headquarters in Newark, New Jersey were stolen in early November 2013 (the "Data Breach"); these laptops contained the PII, PHI, or PII and PHI (collectively, "PII/PHI") of Plaintiffs and Class Members.

3. Horizon disregarded Plaintiffs' and Class Members' privacy rights by intentionally, willfully, recklessly, or negligently failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure. Plaintiffs' and Class Members' PII/PHI was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class Members' PII/PHI was compromised and stolen.

4. Plaintiffs bring this lawsuit on behalf of themselves and all others similarly situated alleging that Defendant violated the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x ("FCRA"); the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2 *et seq.*; the Truth-in-Consumer Contract, Warranty and Notice Act, N.J.S.A. §§ 56:12-14 *et seq.*; breached its contract

with Plaintiffs and Class Members; invaded Plaintiffs' and Class Members' privacy; acted negligently; and was unjustly enriched.

JURISDICTION AND VENUE

5. The Court has subject matter jurisdiction over Plaintiffs' FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction over Horizon because at all relevant times, Horizon conducted (and continues to conduct) substantial business in the District of New Jersey.

6. Venue is proper in the District of New Jersey pursuant to 28 U.S.C. § 1391(b) and (c), because a substantial part, if not all, of the events giving rise to this action occurred in the District of New Jersey, and Horizon resides and conducts substantial business in the District of New Jersey.

PARTIES

7. Plaintiff Courtney Diana ("Diana") is a New Jersey citizen and resident of New Jersey. Diana is a member of a health insurance plan offered by Horizon. She receives the plan through her employer and pays for a portion of the premiums, which are deducted directly from her paycheck. In December 2013, Diana received a letter from Horizon notifying her that her PII/PHI was on the laptop computers stolen and compromised in the Data Breach.

8. Plaintiff Mark Meisel ("Meisel") is a citizen and resident of New Jersey. Meisel was a member of a health insurance plan offered by Horizon from 2011 through in or about October 2012. Any claims that Meisel submitted pursuant to his former health plan with Horizon were submitted and fully paid prior to November 1, 2012. Meisel received a letter from

Horizon in December 2013 notifying him that his PII/PHI was on the laptop computers stolen and compromised in the Data Breach.

9. Plaintiff Karen Pekelney ("Pekelney") is a citizen and resident of New Jersey. She is the wife of Meisel and has been a member of a health insurance plan offered by Horizon since 2011. Pekelney received a letter from Horizon in December 2013 notifying her that her PII/PHI was on the laptop computers stolen and compromised in the Data Breach.

10. Plaintiff Mitchell Rindner ("Rindner") is a citizen and resident of New York. He has been a member of a health insurance plan offered by Horizon through his New Jersey-based employer and union since at least 2011. Rindner learned of the Horizon Data Breach from his co-workers in February 2014, but he was not initially notified by Horizon. Rindner contacted Horizon in February 2014 at which time Horizon confirmed that his PII/PHI, including his social security number and date of birth, was on the laptop computers stolen and compromised in the Data Breach. As a result of the Data Breach, a thief or thieves submitted to the Internal Revenue Service ("IRS") a fraudulent Income Tax Return for 2013 in Rindner's and his wife's names and stole their 2013 income tax refund. Rindner has spent time working with the IRS and law enforcement (including the United States Department of Justice) and incurred other out-of-pocket expenses to remedy the identify theft. Subsequent to the theft of the income tax refund, someone fraudulently attempted to use Rindner's credit card number in an online transaction. Rindner has also been damaged financially by the related delay in receiving his tax refund for 2013, and he was recently denied retail credit because his social security number has been associated with identity theft. It is the usual practice of Rindner to take steps to protect his identity, including but not limited to shredding all documents containing his social security number prior to discarding.

11. Horizon is a health insurance company with approximately 3.7 million members. Horizon is a New Jersey corporation and is headquartered in Newark, New Jersey.

BACKGROUND FACTS

12. Horizon provides health insurance products and services to individuals and employers in New Jersey. Horizon, through its subsidiaries, also provides dental insurance, life insurance, and worker compensation and personal injury protection administrative services.

13. In the regular course of its business, Horizon collects and maintains possession, custody, and control of the PII/PHI of its customers and potential customers.[1] When prospective members enroll in Horizon's health plans, they complete enrollment forms which require them to provide a variety of sensitive information, including their full name, Social Security number, date of birth, sex, full address, home phone, e-mail address, alternative addresses, one's race or ethnicity, the name and address of one's primary care provider, any preexisting conditions, and information regarding coverage under other health insurance plans.

14. According to the Notice of Information Privacy Practices that appears on Horizon's website (hereinafter "Horizon's Privacy Policy"), in providing health insurance coverage, Horizon collects private information concerning the provision and payment of health care from the following sources: (i) information Horizon receives from customers and potential customers on applications, other forms, or websites that Horizon sponsors; (ii) information it obtains from its customers' transactions with it, its affiliates, or others, such as health care

[1] *See* Notice of Information Privacy Practices by Horizon (effective Sept. 23, 2013), available at http://www.horizonblue.com/privacy-policy (last visited Jun. 9, 2014).

providers; and (iii) information it receives from consumer-reporting agencies or others, such as Medicare, state regulators and law enforcement agencies.[2]

15. Horizon collects, handles, and assembles Plaintiffs' and Class Members' PII/PHI in numerous ways, including, among other things: (1) maintaining their PII/PHI for its own files; and (2) submitting their PII/PHI to third parties for the purposes of providing payment for health care services provided to Plaintiffs and Class Members, setting rates for health insurance, and setting rates for the payment of certain health care services.

16. Horizon also assembles Plaintiffs' and Class Members' PII/PHI and transmits it to third-parties for purposes of determining whether Plaintiffs and Class Members are eligible for various medical treatments and the insurance coverage of such treatments.

17. Horizon's Privacy Policy provides, in relevant part, as follows:

> Our employees are trained on the need to maintain your Private Information in the strictest confidence. They agree to be bound by that promise of confidentiality and are subject to disciplinary action if they violate that promise. We also maintain appropriate administrative, technical and physical safeguards to reasonably protect your Private Information.
>
> In addition, in those situations where we rely on a third party to perform business, professional or insurance services or functions for us, that third party must agree to safeguard your Private Information. That business associate must also agree to use it only as required to perform its functions for us and as otherwise permitted by our contract and the law. Finally, if we or our business associate causes a "breach" of privacy as that term is defined under federal law, we will notify you without unreasonable delay of the occurrence. In these ways, we carry out our confidentiality commitments to you.[3]

[2] *Id.*

[3] *Id.*

18. Defendant shares PII/PHI, and other information with a variety of third parties, including suppliers, vendors, health care providers, pharmacies, board members, and other entities.

19. According to Horizon's Privacy Policy, Horizon may use and disclose members' PII/PHI for a variety of purposes, including, but not limited to: (1) payment activities, (2) health care operations activities, (3) health-related activities, (4) treatment, payment, and health care operations activities, including for purposes of their fraud and abuse detection or compliance, (5) public health activities, (6) health oversight agencies, (7) to carry out appropriate and permissible research, (8) to contact members for fundraising purposes, (9) to conduct marketing activities, and (10) to perform other functions and activities permitted by the federal privacy rules.[4]

20. Plaintiffs and Class Members are or were members of Horizon insurance plans and entrusted Horizon with their PII/PHI.

21. Defendant retained its former health insurance plan members' PII/PHI well after such persons were no longer covered under Defendant's health insurance plans.

22. Plaintiffs' and Class Members' PII/PHI was stored by Horizon in unencrypted format on two laptop computers. The PII/PHI on the two laptops included Plaintiffs' and Class Members' names, addresses, dates of birth and, in some cases, Social Security numbers and medical information.

23. The storage of Plaintiffs' and Class Members' PII/PHI in an unencrypted format on two laptop computers was in violation of established industry practices and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

[4] *Id.*

The 2008 Data Breach

24. In early January 2008, Horizon experienced a data breach when an unsecured Horizon laptop computer containing the PII of 300,000 of its insureds was stolen.[5]

25. After the 2008 laptop theft, New Jersey lawmakers called for an investigation of Horizon, noting that "Horizon is one of the state's largest health insurance companies and the major provider of benefits for public employees, many of whom are retired and have moved out of state. . . . It is outrageous that such a security breach could happen, and its repercussions could certainly cross state lines."[6]

26. In response to public concerns about its data protection policies, Defendant stated that it had begun encrypting all desktops, laptops, and portable media devices, a process it anticipated would be complete in March 2008.[7]

27. A September 2008 news article indicated that a spokesman for Defendant has stated that Defendant had taken steps to improve security and was requiring that all computers be fully encrypted.[8]

Additional Laptop Thefts

28. According to incident reports filed with the Newark Police Department, between February 2008 and April 2013, there were at least three additional incidents of laptop theft from

---

[5] *See* Denise Richardson, *Laptop Stolen Containing Data on 300,000 Customers of Horizon Blue Cross/Blue Shield* (Feb. 2, 2008), available at http://www.givemebackmycredit.com/blog /2008/02/ laptop-stolen-containing-data.html (last visited Jun. 9, 2014).

[6] *See Assemblyman Chiusano Says Massive Horizon Identity Theft Warrants State, Federal Investigations* (Jan.30, 2008), available at http://www.highbeam.com/doc/1P3-1421417871.html (last visited Jun. 11, 2014).

[7] Insurer gives lawmakers reassurance of patient-data security, Press of Atlantic City (New Jersey), Feb. 20, 2008.

[8] When sensitive data is lost; Companies taking steps to combat rising problem of security breaches, The Record (Bergen County NJ), Sept. 3, 2008.

Horizon's headquarters. The reports indicate that Horizon used a large number of laptop computers in conducting its business, some of which are assigned to employees and some of which are placed in storage; many of the laptops being equipped with a computer LoJack system for locating a stolen laptop.

29. In November 2008, Horizon learned via a stolen laptop's LoJack system that one of its laptops had been stolen from its headquarters.

30. In December 2008, a laptop was reported stolen from the 11th floor of Horizon's headquarters; the report indicates that Horizon had noticed the laptop was missing as early as April 2008. This laptop also appeared to be equipped with the computer LoJack system.

31. In April 2013, a laptop locked to a docking station within Horizon's headquarters was stolen. This laptop also appeared to be equipped with the computer LoJack system.

The 2013 Data Breach

32. During the weekend of November 1-3, 2013, two laptop computers containing the unencrypted PII/PHI of Plaintiffs and more than 839,000 Class Members were stolen from Horizon's headquarters in Newark, New Jersey. The theft was discovered on Monday, November 4, 2013, when employees returned to work.

33. The facts surrounding the Data Breach demonstrate that the stolen laptop computers were targeted due to the storage of Plaintiffs' and Class Members' highly sensitive and private PII/PHI on them.

34. According to Horizon, it has 24-hour, 7 days a week security at its Newark offices where the Data Breach occurred. When discussing security relating to the Data Breach, Horizon has stated: "[n]o one can gain access to the building without a valid reason for being there. Whoever stole the two laptops was in the building for a legitimate purpose. The laptops were

tethered by cable locks to the employees' workstations. The locks were disabled. Our security cameras did not capture the theft."[9]

35. The stolen laptops had merely been "cable-locked" to employees' workstations, even though cable-locks are easily defeated with common items including office supplies, soda cans, and toilet paper rolls.[10]

36. Horizon does not know the whereabouts of these laptop computers.

37. Despite knowing about the Data Breach since at least November 4, 2013, and despite Horizon's promise in its Privacy Policy that it will "notify you without unreasonable delay" of a breach of security, Horizon delayed notification to its members for more than one month. Horizon did not begin formally notifying Plaintiffs and Class Members of the Data Breach until December 6, 2013—more than one month after the theft of the laptop computers. Horizon issued an announcement stating, in relevant part:

> [T]wo password-protected, unencrypted laptop computers that were cable-locked to employee workstations were stolen from its Newark headquarters during the weekend of November 1, 2013.
>
> Horizon BCBSNJ notified the Newark Police Department on Monday, November 4, 2013 and began a thorough internal investigation upon discovering that the laptops were missing. A detailed review led by outside computer forensic experts has confirmed that the laptops may have contained files with differing amounts of member information, including name and demographic information (e.g., address, member identification number, date of birth), and in some instances, a Social Security number and/or limited clinical information. Due to the way the stolen

[9] *See* Marianne K. McGee, *Unencrypted Laptops Lead to Mega-Breach*, Data Breach Today (Dec. 9, 2013), available at http://www.databreachtoday.com/unencrypted-laptops-lead-to-mega-breach-a-6277 (last visited Jun. 9, 2014).

[10] *See* CIO.com, *Blue Cross: 840,000 Healthcare Records at Risk After Laptop Theft* (Dec. 10, 2013) available at http://www.cio.com/article/744491/Blue_Cross_840_000_Healthcare_Records_at_ Risk_After_Laptop_Theft (last visited Jun. 11, 2014).

> laptops were configured, it is not certain that all of the member information contained on the laptops is accessible.[11]

38. The stolen laptops were password-protected; however, passwords are easily defeated, and encryption best protects PII or PHI on a laptop.[12]

39. A robust international cyber black market exists for PII/PHI.[13]

40. During the intervening period between the Data Breach and December 6, 2013, Plaintiffs' and Class Members' unencrypted PII/PHI could have been bought and sold on the robust international cyber black market—an extant and illicit market representing imminent risk, harm, and damage to Plaintiffs and Class Members. Horizon's conduct placed Plaintiffs' and Class Members' PII/PHI in the well-recognized sphere of harm for such information.

41. On January 27, 2014, several of Horizon's high-ranking executives testified about the Data Breach before the New Jersey Senate Health, Human Services and Senior Citizens Committee.[14] At that hearing, Senator Joseph Vitale stated that he consulted with information

---

[11] *See* Horizon, *Horizon Blue Cross Blue Shield of New Jersey Notifies Members, Offers Protection Following Office Theft* (Dec. 6, 2013), available at http://www.horizonblue.com/about-us/news-overview/company-news/horizon-bcbsnj-notifies-members (last visited Jun. 11, 2014).

[12] *See*, e.g., American Medical Association, *HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information*, http://www.amaassn.org/resources/doc/washington/ hipaa-phi-encryption.pdf (advising that PHI be encrypted).

[13] *See* Shishir Behera, *Cyber Black Market has Robust Infrastructure: Report* (Mar. 26, 2014), available at http://www.business-standard.com/article/current-affairs/cyber-black-market-has-robust-infrastructure-report-114032600054_1.html (last visited Jun. 17, 2014); *see also* ABC News Report, *Your Medical Records May Not Be Private: ABC News Investigation* (Sep. 13, 2012), available at http://abcnews.go. com/ Health/medical -records-private-abc-news-investigation/story?id=17228986 (last visited Jun. 11, 2014).

[14] *See* The Star-Ledger, Susan K. Livio, *NJ Senate Health Panel Grills Horizon BCBS about Stolen Laptops and Data Breach* (Jan. 27, 2014), available at http://www.nj.com/politics/index.ssf/2014/01/nj_ senate_health_ panel_grills_horizon_about_two_stolen _laptops.html (last visited Jun. 9, 2014).

security experts who stated that the protection of the laptops was "very sloppy."[15] Senator Vitale also questioned the length of the credit protection services offered by Horizon in the wake of the Data Breach.[16]

42. At the January 27, 2014 Senate hearing, Horizon confirmed that it had not encrypted all of its computers that contained PII/PHI.[17]

43. Nearly six years after the first security breach, Horizon essentially admitted that it had not taken steps it had promised to take in 2008 to improve the security of its members' PII/PHI, such as encrypting all of its computers. Horizon stated in a December 2013 letter:

> To help prevent something like this from happening in the future, we are strengthening our encryption processes and enhancing our policies, procedures and staff education regarding the safeguarding of company property and member information. Be assured that protecting your information is a priority at Horizon BCBSNJ.

44. In the aftermath of the Data Breach, Horizon allegedly established safeguards to prevent a similar incident in the future—including tougher policies and stronger encryption processes that could have been implemented prior to the Data Breach and prevented it.

Data Breaches Lead to Identity Theft

45. Identity theft occurs when a person's PII is used or attempted to be used without his or her permission to commit fraud or other crimes.[18]

---

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *See* Federal Trade Commission, *Consumer Information: Identity Theft*, available at http://www.consumer.ftc.gov/features/feature-0014-identity-theft (last visited Jun. 9, 2014).

46. Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report"), quantifying the impact of security breaches.[19] According to the Javelin Report, individuals whose PII is subject to a reported security breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud or identity theft.[20]

47. "[T]he range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and [] any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[21] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[22]

48. Victims of identity theft are at serious risk of substantial losses. "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."[23]

---

[19] *See* Javelin Strategy & Research, *Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier*, available at https://www.javelinstrategy.com/news/1314/92/1 (last visited Jun. 16, 2014).

[20] *Id.*

[21] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, at 8 (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited Jun. 9, 2014).

[22] *Id.* at 20.

[23] *See* Federal Trade Commission, *Signs of Identity Theft*, available at http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited Jun. 9, 2014).

49. Theft of medical information, such as that included in the Data Breach here, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[24]

50. Identity thieves also use Social Security numbers to commit other types of fraud. Identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft can be the most damaging because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

51. Identity thieves also use Social Security numbers to obtain false identification cards, obtain government benefits in the victim's name, commit crimes, and file fraudulent tax returns to obtain fraudulent tax refunds. Identity thieves also obtain jobs, rent houses and apartments, and obtain medical services in the victim's name using stolen Social Security numbers. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an

[24] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles /0171-medical-identity-theft (last visited Jun. 9, 2014).

unwarranted criminal record. Victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well as the damage to their "good name."[25]

52. The unauthorized disclosure of a person's Social Security number can be particularly damaging because Social Security numbers cannot be easily replaced. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[26] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

53. Obtaining a new Social Security number also is not a complete remedy for identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

54. PII/PHI, such as Plaintiffs' and Class Members' PII/PHI on the stolen laptops, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[27]

---

[25] *See* Government Accounting Office, *Governments Have Acted to Protect Personally Identifiable Information, But Vulnerabilities Remain* (Jun. 17, 2009), available at http://www.gao.gov/new.items/ d09759t.pdf (last visited Jun. 9, 2014).

[26] *See* Social Security Administration, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064, October 2007, ICN 46327, available at http://www.ssa.gov/ pubs/10064.html (last visited Jun. 9, 2014).

[27] Companies also recognize PII and PHI as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

Identity thieves and other cyber criminals openly post stolen credit card numbers, Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available. In one study, researchers found hundreds of websites displaying stolen personal financial information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[28]

55. It is reported that "medical records hold an average black market value of $50 per record."[29]

Plaintiffs and Class Members Suffered Damages

56. The Data Breach was a direct and proximate result of Horizon's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Horizon's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/PHI to protect against reasonably foreseeable threats to the security or integrity of such information.

57. Plaintiffs' and Class Members' PII/PHI is private and sensitive in nature and was left inadequately protected and unencrypted by Horizon. Horizon did not obtain Plaintiffs' and

---

[28] *See* StopTheHacker, *The Underground Credit Card Blackmarket*, available at http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Jun. 9, 2014).

[29] Pamela Louis Dolan, *Health Data Breaches Usually Aren't Accidents Anymore* (July 29, 2013), available at http://www.amednews.com/article/20130729/business/130729953/4/ (last visited Jun. 9, 2013).

Class Members' consent to disclose their PII/PHI to any other person as required by HIPAA and other pertinent laws, regulations, industry standards, and internal company standards..

58. As a direct and proximate result of Horizon's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft, identity fraud, and medical fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, placing "freezes" and "alerts" with the credit reporting agencies, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports, accounts, and explanations of benefits from Horizon for unauthorized activity. Because Plaintiffs' and Class Members' Social Security numbers were stolen and compromised, as well as their medical information, they also now face a significantly heightened risk of identity theft, identity fraud, and medical fraud.

59. Horizon's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' unencrypted PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a) actual identity fraud or identity theft;

b) the untimely and inadequate notification of the Data Breach;

c) improper disclosure of their PII/PHI;

d) loss of privacy;

e) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of identity theft, identity fraud, and medical fraud;

f) ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to mitigate or to avert the increased risk of identity theft, identity fraud, and medical fraud;

g) ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market; [30]

h) ascertainable losses in the form of economic injury stemming from Horizon's failure to secure their PII/PHI which they paid for as part of their monthly premiums;

i) deprivation of rights they possess under FCRA; and

j) deprivation of rights they possess under the New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-1 et seq.

60. For example, Plaintiff Rindner has spent time working with the IRS and law enforcement (including the United States Department of Justice) to remedy the effects of the fraudulent Income Tax Return and stolen tax refund and incurred other out-of-pocket expenses to remedy the identify theft. Rindner has also been damaged financially by the related delay in receiving his tax refund for 2013, and was recently denied retail credit because his social security number has been associated with identity theft.

[30] *See, e.g.*, John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

61. Damages can also be ascertained and measured by the average black market prices for Plaintiffs' PII/PHI. For example, medical records hold an average black market value of $50 per record.

62. Notwithstanding Horizon's wrongful actions and inaction and the resulting Data Breach, Horizon has offered only one year of credit monitoring and identity theft protection services through Experian's ProtectMyId Alert. This offer is insufficient because, *inter alia*, it does not address many categories of damages being sought. The cost of adequate and appropriate coverage, or insurance, against the loss position Horizon has placed Plaintiffs and Class Members in, is ascertainable and is a determination appropriate for the trier of fact.

63. The Experian ProtectMy ID service offered does not address the following issues:

a) Credit monitoring through Experian only protects a consumer if a lender pulls a credit report from Experian before extending credit. If a lender instead pulls a report from Trans Union or Equifax, ProtectMyID Alert may not protect the consumer.[31]

b) Even if fraud is detected, a person still must place "freezes" and "alerts" with the other two credit bureaus (TransUnion and Equifax), close or modify financial accounts, and closely review and monitor their credit reports, accounts, and explanations of benefits from Horizon for unauthorized activity.

c) Additionally, the PII/PHI could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection is up.

[31] Claudia Buck, *Target credit monitoring not enough, experts say*, Columbus Dispatch (Apr. 27, 2014), http://www.dispatch.com/content/stories/business/2014/04/27/target-credit-monitoring-not-enough-experts-say.html (last visited Jun. 25, 2014).

d) Although ProtectMyID will check a consumer's credit report on a daily basis for new accounts and other reportable transactions, it does not monitor misuse of existing financial accounts or medical identity unless such misuse results in a new loan or other transaction that would appear on a credit report.[32] As a result, ProtectMyID may not detect all misuse of a consumer's PII or PHI, or it may detect misuse well after significant harm has occurred.

64. PHI may contain information about a consumer's personal life, such as lifestyle, fitness, diseases, and possibly genetic information, all of which could be used to impersonate victims or possible blackmail individuals in public positions—harms that ProtectMyID does not protect against.[33]

65. Theft of medical information, such as that included in the Data Breach here, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[34]

---

[32] *See* http://www.protectmyid.com/EXPERIAN/faq/ (last visited Jun. 12, 2014), *see also* http://www.protectmyid. com/EXPERIAN/our-product-benefits/ (last visited Jun. 12, 2014).

[33] *See* LorenzoFranceschi-Bicchiera, *Healthcare Data of 840,000 at Risk After Laptop Theft* (Dec. 19, 2013), available at http://mashable.com/2013/12/19/horizon-blue-cross-blue-shield-laptop-theft/ (last visited Jun. 12, 2014).

[34] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Dec. 4, 2013).

CLASS ACTION ALLEGATIONS

66. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this class action as a national class action on behalf of themselves and the following Class of similarly situated individuals:

> All persons whose personal identifying information (PII) or protected health information (PHI) were contained on the computers stolen from Horizon's Newark, New Jersey office on or about November 1-3, 2013.

Excluded from the Class are (i) Horizon owners, officers, directors, employees, agents, and representatives and its parent entities, subsidiaries, affiliates, successors, and assigns; and (ii) the Court, Court personnel, and members of their immediate families.

67. The putative Class comprises over 839,000 persons, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

68. The rights of each Class Member were violated in a virtually identical manner as a result of Horizon's willful, reckless, or negligent actions and inaction.

69. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) whether Horizon violated FCRA by failing to properly secure Plaintiffs' and Class Members' PII/PHI;

b) whether Horizon violated FCRA by failing to encrypt Plaintiffs' and Class Members' PII/PHI;

c) whether Horizon willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class Members' PII/PHI;

d) whether Horizon was negligent in storing and failing to protect Plaintiffs' and Class Members' PII/PHI;

e) whether Horizon owed a duty to Plaintiffs and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

f) whether Horizon breached its duty to exercise reasonable care in protecting and securing Plaintiffs' and Class Members' PII/PHI;

g) whether by publicly disclosing Plaintiffs' and Class Members' PII/PHI without authorization, Horizon invaded Plaintiffs' and Class Members' privacy;

h) whether Horizon has been unjustly enriched in the form of premiums paid by Plaintiffs and Class Members that were, in part, paid for the purpose of securing and safeguarding Plaintiffs' and Class Members' PII/PHI;

i) whether Horizon violated the New Jersey Consumer Fraud Act;

j) whether Horizon violated the Truth-In-Consumer Contract, Warranty and Notice Act;

k) whether Plaintiffs and Class Members sustained damages as a result of Horizon's failure to secure and protect their PII/PHI; and

l) whether Horizon violated federal and state laws by failing to timely notify Plaintiffs and Class Members on an individual basis about the theft and dissemination of their PII/PHI.

70. Plaintiffs' claims are typical of Class Members' claims in that Plaintiffs' claims and Class Members' claims all arise from Horizon's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/PHI and the resulting Data Breach.

71. Plaintiffs and their counsel will fairly and adequately represent the interests of Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, Class Members' interests. Plaintiffs' attorneys are highly experienced in the prosecution of consumer class actions and data breach class actions, and intend to vigorously prosecute this action on behalf of Plaintiffs and Class Members.

72. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been

irreparably harmed as a result of Horizon's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Horizon's failure to secure and protect Plaintiffs' and Class Members' PII/PHI.

73. Class certification, therefore, is appropriate pursuant to Fed. R. Civ. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

74. Class certification also is appropriate pursuant to Fed. R. Civ. P. 23(b)(2) because Horizon has acted or refused to act on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole.

75. Class certification also is appropriate because the expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

COUNT I

Willful Violation of the Fair Credit Reporting Act

76. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

77. One of the fundamental purposes of FCRA is to protect consumers' privacy. 15 U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential. 15 U.S.C. § 1681(b).

78. FCRA defines a "consumer reporting agency" as:

> [A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of

> interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

79. FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

80. On a cooperative nonprofit basis or for monetary fees, Defendant regularly assembles consumer information including, among other things, insurance policy information, such as names, dates of birth, and Social Security Numbers of those insured; claims information, such as the date of loss, type of loss, and amount paid for claims submitted by an insured; and a description of insured items. Defendant also regularly utilizes interstate commerce to furnish such information on consumers (consumer reports) to third parties. For example:

> We routinely use and disclose Private Information in connection with your health care coverage, to determine your eligibility for coverage and benefits, and to see that the treatment and services you receive are properly billed and paid. To do this, we may share Private Information with health care providers, their billing agents, insurance companies and others. Our payment activities can also include the use of Private Information for: risk adjustment, billing, claims management, collection activities, utilization review, medical necessity determinations, drug rebate contract reporting of drug utilization, underwriting and other rate-setting activities.[35]

[35] *See* Notice of Information Privacy Practices by Horizon (effective Sept. 23, 2013), available at http://www.horizonblue.com/privacy-policy (last visited Jun. 9, 2014).

81. Plaintiffs' and Class Members' PII/PHI constitute Consumer Reports under FCRA, because this information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiffs' and the other Class Members' eligibility for insurance to be used primarily for personal, family, or household purposes, and establishing rates for same.

82. FCRA requires the adoption of reasonable procedures with regard to, inter alia, the confidentiality and proper utilization of personal and insurance information. 15 U.S.C. § 1681(b). FCRA also requires that consumer reporting agencies "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e.

83. Defendant failed to adopt and maintain these and other reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b. In addition to properly securing and monitoring the stolen laptop computers and encrypting Plaintiffs' and Class Members' PII/PHI on the computers, accepted industry practice dictates Horizon should have taken the following measures:

a) Conducted periodic risk assessments and gap analysis relating to privacy and information security-related policies, processes and procedures. A comprehensive risk analysis would have identified the (i) physical vulnerability of Horizon's locations, (ii) administrative vulnerabilities associated with storing over 839,000 members' PII/PHI on two laptop computers, and (iii) technical vulnerabilities, including the need to restrict unauthorized access and encrypt at-risk data;

b) Developed privacy and information security related performance and activity metrics, such as the performance of ongoing compliance reviews, physical walkthroughs, hotline and complaint management—and ensure that these metrics were an integral part of Horizon's corporate governance program; and

c) Taken measures to monitor and secure the room and areas where the laptop computers containing the PII/PHI were stored, maintained, and used, or taken measures to insure that no PII/PHI was stored on unencrypted portable electronic devices.

84. On information and belief, Horizon failed to take reasonable and appropriate measures to secure the stolen laptop computers and safeguard and protect Plaintiffs' and Class Members' PII/PHI. Horizon also failed to place itself in a position to immediately notify Plaintiff and Class Members about the Data Breach.

85. FCRA defines "medical information" as:

> [I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to—(A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual.

15 U.S.C. § 1681a(i).

86. FCRA specifically protects medical information, restricting its dissemination to limited instances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

87. Plaintiffs' and Class Members' PHI affected by the Data Breach constitutes medical information as defined by FCRA. Their PHI included enrollment and clinical information, which constitute data relating to the provision of health care and past, present, or future physical, mental, or behavioral health or condition of an individual under FCRA's definition of medical information. *See* 15 U.S.C. § 1681a(i).

88. Under FCRA, a "person that receives medical information [in connection with the business of insurance or annuities] shall not disclose such information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or

as otherwise permitted by statute, regulation, or order." 15 U.S.C. §§ 1681b(g)(4), 1681b(g)(3)(A).

89. Under FCRA, the business of insurance includes "the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners (as in effect on January 1, 2003)." 15 U.S.C. § 1681b(g)(3)(A). Section 18B of the model Privacy of Consumer Financial and Health Information Regulation includes such activities as claims administration, claims adjustment and management, underwriting, policy issuance, case management, and disease management; these are activities in which Horizon engages.

90. Because Horizon is a person that receives medical information in connection with the business of insurance, under FCRA, Horizon shall not disclose such information to any other person except as necessary to carry out the purpose for which it received the information or as permitted by statute, regulation, or order. *See* 15 U.S.C. §§ 1681b(g)(4), 1681b(g)(3)(A).

91. Horizon's failure to protect and safeguard the PII/PHI of Plaintiffs and Class Members resulted in the disclosure of such information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Horizon received the information, nor was it permitted by statute, regulation, or order.

92. Defendant's violations of FCRA, as set forth above, were willful or, at the very least, reckless, constituting willfulness. In light of the 2008 laptop theft and Defendant's ensuing assurances that it would encrypt all laptops, Defendant's failure to encrypt or otherwise adequately protect Plaintiffs' and Class Members' PII/PHI was willful.

93. As a result of Defendant's willful or reckless failure to adopt and maintain reasonable procedures to limit the furnishing of Plaintiffs' and Class Members' PII to the

purposes listed under 15 U.S.C. § 1681b, Plaintiffs' and the other Class Members' PII was disseminated to unauthorized third parties, compromised, and stolen. Plaintiffs suffered individual harm as a result of Defendant's willful or reckless violations of FCRA.

94. As a further direct or proximate result of Defendant's willful or reckless violations of FCRA, as described above, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint.

95. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages (as described in detail in paragraphs 56-65 of this Consolidated Class Action Complaint) or statutory damages of not less than $100, and not more than $1,000, each, as well as attorneys' fees, punitive damages, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

COUNT II

Negligent Violation of the Fair Credit Reporting Act

96. Plaintiffs repeat and re-allege paragraphs 1 through 91 as if fully set forth herein.

97. Defendant negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

98. Plaintiffs' and the other Class Members' PII/PHI was wrongfully disseminated to the public as a direct and foreseeable result of Defendant's failure to adopt and maintain such reasonable procedures.

99. Horizon disclosed medical information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Horizon received the information, nor was it permitted by statute, regulation, or order.

100. As a direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs' and Class Members' PII/PHI was made accessible to unauthorized third parties in the public domain, compromised, and stolen. Plaintiffs suffered individual harm as a result of Defendant's negligent violations of FCRA.

101. As a further direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint.

102. Plaintiffs and the other Class Members, therefore, are entitled to compensation for their actual damages (as described in detail in paragraphs 56-65 of this Consolidated Class Action Complaint), as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o.

COUNT III

Negligence

103. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

104. Defendant had a duty to exercise reasonable care to protect and secure Plaintiffs' and the Class Members' PII/PHI.

105. Through its acts and omissions, Defendant violated its duty to use reasonable care to protect and secure Plaintiffs' and Class Members' PII/PHI as follows:

a) Defendant failed to encrypt or otherwise electronically protect and secure Plaintiffs' and Class Members' PII/PHI;

b) Defendant failed to physically protect and secure Plaintiffs' and Class Members' PII/PHI; and

c) Defendant retained Plaintiffs' and Class Members' PII/PHI longer than was reasonably necessary.

106. It was reasonably foreseeable that Defendant's failure to exercise reasonable care to protect and secure Plaintiffs' and Class Members' PII/PHI would result in an unauthorized third party gaining access to, possession of, and control over such information for an unlawful purpose, particularly where Defendant previously experienced laptop thefts, including the theft of a laptop containing its members' PII.

107. Even without the previous multiple laptop thefts and Defendant's assurances that it would encrypt all laptops, Defendant's failure to encrypt or otherwise adequately protect Plaintiffs' and Class Members' PII/PHI was negligent, with the previous thefts underscoring the severity of Defendant's conduct.

108. Plaintiffs' and Class Members' PII/PHI constitute personal property and due to Defendant's negligence their PII/PHI was stolen, resulting in harm to Plaintiffs and Class Members.

109. Horizon's negligence directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' unencrypted PII/PHI and Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint.

COUNT IV

Breach of Contract

110. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

111. Defendant provides health insurance to Plaintiffs and Class Members pursuant to insurance contracts:

a) Plaintiffs and Class Members were either parties to, or third-party beneficiaries of, these insurance contracts.

b) As consideration under the insurance contracts, Plaintiffs and Class Members paid or had paid on their behalf insurance premiums, amounting to thousands of dollars paid annually by or on behalf of each plan member.

c) These insurance contracts explicitly or implicitly incorporate statements made in Horizon's Privacy Policy or on its website that Defendant would safeguard and protect Plaintiffs' and Class Members' PII/PHI. Horizon's Privacy Policy states: "We also maintain appropriate administrative, technical and physical safeguards to reasonably protect your Private Information."

112. Pursuant to their insurance contracts, Plaintiffs and Class Members paid Defendant to, *inter alia*, safeguard and protect their PII/PHI.

113. Defendant did not safeguard or protect Plaintiffs' and Class Members' PII/PHI as required by the insurance contracts.

114. Because Defendant did not safeguard and protect Plaintiffs' and Class Members' PII/PHI as promised, Plaintiffs and Class Members overpaid for their insurance premiums and have been (and continue to be) damaged.

115. Because Defendant did not safeguard and protect Plaintiffs' and Class Members' PII/PHI as promised, Plaintiffs and Class Members did not receive the full value of their insurance contracts and have been (and continue to be) damaged

116. Additionally, as a result of Defendant's breach of contract, Plaintiffs and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint.

COUNT V

Invasion of Privacy

117. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

118. Plaintiffs' and Class Members' PII/PHI is private information.

119. Dissemination and publication of Plaintiffs' and Class Members' PII/PHI would be offensive to a reasonable person.

120. The public has no legitimate interest in being apprised of Plaintiffs' and Class Members' PII/PHI.

121. Defendant's failure to safeguard and protect Plaintiffs' and Class Members' PII/PHI directly and proximately resulted in unreasonable publicity to the private lives of Plaintiffs and Class Members.

122. Plaintiffs' and Class Members' have a legal interest in the privacy of their PII/PHI.

123. Defendant's failure to safeguard and protect Plaintiffs' and Class Members' PII/PHI was a direct and proximate cause of the access to the PII/PHI and the obtaining of the PII/PHI as a matter of law.

124. Defendant's failure to safeguard and protect Plaintiffs' and Class Members' PII/PHI deprived Plaintiffs and Class Members of their legal interest in the privacy of that information, causing them damages.

125. As a result of Defendant's actions and inactions resulting in Plaintiffs' and Class Members' loss of privacy, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint.

COUNT VI

Unjust Enrichment

126. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

127. Plaintiffs and Class Members are either parties to, or third-party beneficiaries of, insurance contracts with Defendant.

128. Plaintiffs and Class Members conferred a benefit on Defendant by paying health insurance premiums to Defendant, a portion of which covered the administrative costs associated with protecting its members' PII/PHI.

129. Defendant has been unjustly enriched in retaining the portion of Plaintiffs' and Class Members' premiums that covered the administrative costs associated with protecting its members' PII/PHI.

130. It would be inequitable for Defendant to retain the portion of Plaintiffs' and Class Members' premiums that covered the administrative costs associated with protecting its members' PII/PHI because Defendant misrepresented that it was protecting and safeguarding its members' PII/PHI when in fact it was not, causing injuries to Plaintiffs and all Class Members.

131. Plaintiffs seek restitution or disgorgement of Defendant's ill-gotten gains.

132. Additionally, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint, and seek restitution related to same.

COUNT VII

Unlawful Practice in Violation of the New Jersey Consumer Fraud Act, N.J.S.A. §§ 56:8-2 *et seq.*

133. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

134. The New Jersey Consumer Fraud Act defines merchandise as "any objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale." N.J.S.A. § 56:8-1(c).

135. The health insurance plans sold by Defendant to Plaintiffs and members of the proposed Class constitute merchandise under the New Jersey Consumer Fraud Act.

136. Under the New Jersey Consumer Fraud Act, the following qualifies as an unlawful practice:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.

N.J.S.A. § 56:8-2.

137. In enacting the Identity Theft Prevention Act, which among other things, amended the New Jersey Consumer Fraud Act, the New Jersey Legislature found that"[i]dentity theft is an act that violates the privacy of our citizens and ruins their good names: victims can

suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories." N.J.S.A. § 56:11-45.

138. Defendant's 2008 public promise to encrypt all computers and privacy policy promising to protect members' PII/PHI constitute an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation because Defendant knew that it had not encrypted all of its computers and had not adopted other adequate electronic or physical safeguards to safeguard its members' PII/PHI.

139. Plaintiffs and Class Members had a reasonable expectation that Defendant's 2008 public promise to encrypt all computers and privacy policy, promising to protect members' PII/PHI had been fulfilled and the failure to do so constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation in violation of N.J.S.A. § 56:8-2.

140. Horizon's Privacy Policy states: "We also maintain appropriate administrative, technical and physical safeguards to reasonably protect your Private Information. This statement constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation because Defendant knew that it had not maintained appropriate administrative, technical, and physical safeguards to protect its members PII/PHI.

141. Plaintiffs and Class Members had a reasonable expectation that Horizon would abide by the terms of its Privacy Policy, and the failure to do so constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation in violation of N.J.S.A. § 56:8-2.

142. Defendant had a duty to advise Plaintiffs and Class Members that it had not encrypted all computers and that its data security was inadequate, and by not doing so, concealed, suppressed, or omitted material facts.

143. Defendant intended for Plaintiffs and the members of the proposed Class to rely upon the concealment, suppression, or omission of material fact relating to its data security when they entered into or renewed their health insurance contracts with Defendant.

144. Plaintiffs and Class Members had a reasonable expectation that their PII/PHI had been encrypted and that data security was adequate when they entered into and renewed their health insurance contracts with Defendant.

145. Plaintiffs and Class Members would not have enrolled or renewed their health insurance contracts with Defendant if Defendant had not concealed, suppressed, or omitted the material fact relating to Defendant's data security.

146. Defendant's actions constitute a knowing, concealment, suppression, or omission in violation of N.J.S.A. § 56:8-2.

147. As a result of the foregoing, Plaintiffs and Class Members suffered and will continue to suffer ascertainable losses and other damages as described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint, and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

COUNT VIII

Failure to Destroy Certain Records in Violation of N.J.S.A. § 56:8-162

148. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

149. The New Jersey Consumer Fraud Act provides that it is "an unlawful practice and a violation of P.L. 1960, c. 39 (c. 56:8-1 et seq.) to willfully, knowingly or recklessly violate" Sections 56:8-161-164 of that Act.

150. Section 56:8-162 of the New Jersey Consumer Fraud Act requires that a business "destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means." N.J.S.A. § 56:8-162.

151. In violation of N.J.S.A. § 56:8-162, Defendant retained its former customers' PII/PHI well after such persons were no longer covered under Defendant's health plans.

152. Once a laptop is stolen from Horizon, any PII/PHI on that laptop is no longer retained by Horizon; thus, Horizon has a duty under § 56:8-162 of the New Jersey Consumer Fraud Act to destroy such data.

153. There are technologies available that automatically wipe mobile devices, such as laptops, if they leave a geographic area. Because Horizon failed to employ any technologies to destroy the PII/PHI contained on the laptops stolen in November 2013, Horizon has violated § 56-8-162 of the New Jersey Consumer Fraud Act.

154. As a result of the foregoing, Plaintiffs and Class Members suffered and will continue to suffer ascertainable losses and other damages as described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint, and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

COUNT IX

Failure to Expediently Notify Following Security Breach
in Violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-2 et seq.

155. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

156. As stated above, the New Jersey Consumer Fraud Act provides that it is "an unlawful practice and a violation of P.L. 1960 c. 39 (C.56:8-1 *et seq*.) to willfully, knowingly or recklessly violate" Sections 56:8-161-164 of that Act.

157. Section 56:8-163 of the New Jersey consumer Fraud Act requires that a business conducting business in New Jersey:

> shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

N.J.S.A. § 56:8-163.

158. The New Jersey Consumer Fraud Act defines a breach of security as follows:

> "Breach of security" means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56:8-161.

159. The 2013 theft of the laptops from Defendant's headquarters constituted a breach of security.

160. Defendant's disclosure regarding the breach of security to Plaintiffs and Class Members was delayed and not made in the most expedient time possible.

161. As a result of the foregoing, Plaintiffs and Class Members suffered and will continue to suffer ascertainable losses and other damages as described in detail in paragraphs 56 through 65 of this Consolidated Class Action Complaint, and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

COUNT X

Truth-in-Consumer Contract, Warranty and Notice Act

162. Plaintiffs repeat and re-allege paragraphs 1 through 75 as if fully set forth herein.

163. The New Jersey Truth-in Consumer Contract, Warranty and Notice Act, N.J.S.A. §§ 56:12-14 *et seq.* ("TCCWNA"), prohibits a seller, lessor, creditor, lender or bailee from offering or giving written contracts or notices to consumers that contain any provision that violates consumer rights or the responsibilities of the seller, lessor, creditor, lender or bailee under clearly established New Jersey or federal law. N.J.S.A.§ 56:12-15.

164. The TCCWNA defines "consumer" as "any individual who buys, leases, borrows, or bails any money, property or service which is primarily for personal, family or household purposes." N.J.S.A. § 56:12-15.

165. Plaintiffs and Class Members are consumers protected by the TCCWNA, because they bought insurance from Horizon.

166. Horizon is a "seller" governed by the provisions of the TCCWNA because it sold insurance to Plaintiffs and Class Members.

167. Horizon's Privacy Policy is an actionable notice under the TCCWNA, because it is a written announcement that Horizon adequately safeguards its customers' private information.[36]

168. The Data Breach constitutes willful or negligent violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681n(a). The data breaches violate Plaintiffs' clearly-established right under FCRA to having their personal, private information kept confidential by Horizon. In light of the 2008 laptop threat and Horizon's ensuing assurances that it would encrypt *all* laptops, Horizon's failure to encrypt or otherwise adequately protect the confidentiality of members' PII/PHI constituted a violation of 15 U.S.C. § 1681(b).

169. The Data Breach constitutes a violation of the New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-1 *et seq.*, and a violation of Plaintiffs' clearly-established right to not be defrauded by misrepresentations or unconscionable practices by Horizon. Horizon's Privacy Policy constituted misrepresentations and the failure to encrypt laptops with members' PII/PHI constitute unconscionable practices in violation of the CFA.

170. Given these predicate statutory violations—violating the clearly established rights of Plaintiffs to have their personal information encrypted and protected—both under FCRA and the CFA—Horizon violated the TCCWNA. Pursuant to the TCCWNA, Horizon is therefore liable to Plaintiffs and the Class for statutory damages for each violation of TCCWNA under N.J.S.A. § 56:12-17.

[36] *See* Notice of Information Privacy Practices by Horizon (effective Sept. 23, 2013), available at http://www.horizonblue.com/privacy-policy (last visited Jun. 9, 2014).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for entry of an Order:

a. certifying the Class, appointing Plaintiffs as Class Representatives, and appointing Ben Barnow of Barnow and Associates, P.C.; Philip A. Tortoreti of Wilentz, Goldman & Spitzer, P.A.; Laurence D. King of Kaplan Fox & Kilsheimer LLP; and Joseph J. DePalma of Lite DePalma Greenberg, LLC, as Co-Lead Class Counsel;

b. requiring Defendant to take steps to ensure that its members' PHI and PII are adequately protected;

c. awarding Plaintiffs and the other Class Members statutory, actual, and other applicable damages, including punitive damages;

d. enjoining Defendant from continuing to store PII and PHI in an unencrypted manner;

e. awarding Plaintiffs and Class Members pre-judgment and post-judgment interest;

f. requiring Defendant to reimburse Plaintiffs and other Class Members for their ascertainable losses;

g. awarding Plaintiffs and Class Members reasonable attorneys' fees and costs of suit, including expert witness fees; and

h. awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable as a matter of right.

Dated: June 27, 2014

Respectfully submitted,

WILENTZ, GOLDMAN & SPITZER P.A.
90 Woodbridge Center Drive
Suite 900, Box 10
Woodbridge, New Jersey 07095-0958
Telephone: (732) 636-8000
Email: ptortoreti@wilentz.com

/s/ Philip A. Tortoreti
Philip A. Tortoreti

Ben Barnow (admitted *pro hac vice*)
BARNOW AND ASSOCIATES, P.C.
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
Email: b.barnow@barnowlaw.com

Joseph J. DePalma
Lite DePalma Greenberg, LLC
Two Gateway Center, Suite 1201
Newark, NJ 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
Email: jdepalma@litedepalma.com

Laurence D. King (admitted *pro hac vice*)
Kaplan Fox & Kilsheimer LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
Email: lking@kaplanfox.com

Plaintiffs' Interim Co-Lead Counsel

Robert N. Kaplan
David A. Straite
Lauren I. Dubick
KAPLAN FOX & KILSHEIMER LLP
850 3rd Avenue, 14th Floor
New York, New York 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
rkaplan@kaplanfox.com
dstraite@kaplanfox.com
ldubick@kaplanfox.com

Additional Plaintiffs' Counsel